REMARKS

Claims 1-32 are pending in the present application

This Amendment is in response to the Final Office Action mailed September 24, 2008. In the Final Office Action, the Examiner rejected claims 1-14, 10-13, 18-23, 27, and 28 under 35 U.S.C. §102(b) and claims 15-17, 24-26 and 29-32 under 35 U.S.C. §103(a). Reconsideration in light of the remarks made herein is respectfully requested.

On November 30, 2007, the undersigned attorney conducted a telephone conference and discussed what elements of U.S. Patent No. 6,289,455 (Kocher) were construed as the "first value", the "second value" and the "third value" as set forth in claims 1 and 14. The Examiner identified that the "rights key", "KDM" and "CDK" were interpreted by him to constitute the "first value", the "second value" and the "third value," respectively.

Formal Request for Examiner's Interview

Applicant respectfully requests the Examiner to contact the undersigned attorney to discuss the allowability of the pending claims especially if, after his review, there are still outstanding rejections regarding patentability. The undersigned attorney can be reached at the telephone number listed below.

Rejection Under 35 U.S.C. § 102

Claims 1-14, 18-23, 27 and 28 were rejected under 35 U.S.C. §102(b) as being anticipated by Kocher (Patent No. 6,289,455). Applicant respectfully requests the Examiner to withdraw this rejection because a *prima facie* case of anticipation has not been established.

As the Examiner is aware, to anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Vergegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the…claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989). Herein, all of the claim limitations are not found in Kocher.

A. Claim 1

For instance, with respect to claim 1, the Office Action does not clearly identify the elements set forth in the claims. However, based on the Examiner's interview conducted on November 30, 2007, the undersigned attorney conducted a telephone conference and discussed what elements of U.S. Patent No. 6,289,455 (Kocher) were construed as the "first value", the "second value" and the "third value" as set forth in claims 1 and 14. The Examiner identified that the "rights key", "KDM" and "CDK" were interpreted by him to constitute the "first value", the "second value" and the "third value," respectively.

Applicant respectfully disagrees that the "rights key", "KDM" and "CDK" disclose the "first value", the "second value" and the "third value," respectively, as delineated in claim 1.

Claim 1 recites, among other things, "a control word key ladder logic to produce (i) a first value generated based on a conditional access (CA) random value and the unique key, (ii) a second value generated using the first value, and (iii) a third value recovered by a cryptographic operation using the second value; a first cryptographic unit to descramble incoming content in a scrambled format based on the third value; and a second cryptographic unit to decrypt incoming encrypted data using the first value."

As described at column 11, lines 40-63 of Kocher, the interface control processor (ICP) uses the key derivative message (KDM) to obtain a content decryption key (CDK) generator value. The CDK generator value may be an encrypted form of the CDK and part of the KDM. The KDM can identify whether the rights key is appropriate for processing each CDK generator. *However, the KDM (second value) is not generated using the rights key (first value). Emphasis added.* In contrast, the CDK generator is transformed by the rights key using pseudo-asymmetric function F_3 and the ICP produces the final CDK from the F_3 result.

Additionally, the Examiner alleges that "the rights keys *[first value]* are used to derive the CDK's which are part of the KDM *[second value]*" (Final Office Action, page 8) such that the rights keys are thus used to generate the KDM (Final Office Action, page 8). Applicant respectfully disagrees.

Kocher merely discloses that the CDK generator is an encrypted form of the CDK and is part of the KDM (Kocher, col. 11, lines 41-43). Using the rights key, the CDK generator is transformed to produce the F_3 result which is subsequently used to produce the final CDK

(Kocher, col. 11, lines 40-63). While the final CDK is derived using the rights keys, Applicant respectfully submits that it is false to conclude that the KDM is generated using the rights keys merely because it includes the CDK generator from which the CDK is derived. Therefore, Kocher fails to describes control word key ladder logic to provide a second value, allegedly KDM, generated using the first value, allegedly the rights key.

Additionally, claim 1 includes the limitation of a second cryptographic unit to decrypt incoming encrypted data using a first value, allegedly the rights key. The "rights key" is a derivation of the content identifier for use in post-payment processing (Kocher, col. 11, lines 6-23) The rights key, however, is not used for decryption of incoming encrypted data.

Hence, Applicant respectfully submits that claim 1 is in condition for allowance.

B. Claim 13

Similarly, with respect to claim 13, the Examiner has advised the undersigned attorney that he has construed the "rights key", "KDM" and "CDK" as the "first value", "second value" and "third value," respectively.

Applicant incorporates by reference the arguments set forth above.

Additionally, claim 13 recites, among other things, "a second value recovered from a mating key generator undergoing a cryptographic operation using the first value where the mating key generator is a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number." *Emphasis Added.*

Applicant further traverses the rejection because a second value, allegedly KDM, is not recovered from a mating key generator undergoing a cryptographic operation using the first value, allegedly the rights key. Kocher merely teaches that KDM is "a message generated by a content provider... KDMs are usually transmitted with…corresponding content" (Kocher, col. 8, lines 17-20). The ICP receives a KDM from the playback device (Kocher, col. 11, lines 38-40; Figure 5).

Therefore, since the KDM is merely generated by a content provider and received from the playback device, there is no teaching or suggestion that the KDM is recovered from a mating key generator, let alone, a mating key generator which "is a message that comprises at least one

of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number" as delineated in the claim.

Hence, Applicant respectfully submits that claim 13 is in condition for allowance.

C. Claim 22

With respect to independent claim 22, the Examiner appears to have construed the "rights key", "KDM" and "CDK" as the "first derivative key", "mating key" and the "control word," respectively. Applicant respectfully traverses the rejection because claim 22 includes at least two claim limitations that are not taught by Kocher, namely:

> "a second process block configured to generate a mating key from a mating key generator using the first derivative key, the mating key generator being a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number, and
>
> a third process block configured to recover a control word by decrypting an encrypted control word using the mating key."

As claimed, Applicant respectfully disagrees that the second process block, namely the process to access content as described on column 11 (lines 35-45) of Kocher, is configured to generate a mating key (KDM) from a mating key generator using the first derivative key (rights key).

As discussed above, the rights key has no involvement in the generation of the KDM. The Examiner alleges that "the rights keys (i.e. first derivative keys) are used to derive the CDKs which are part of the KDM (i.e. mating key). Therefore, Kocher discloses the first derivative key is used to generate a mating key" (Final Office Action, page 8). Applicant respectfully disagrees. As above, while the final CDK is derived using the rights keys, Applicant respectfully submits that it is false to conclude that the KDM is generated using the rights keys merely because it includes the CDK generator from which the CDK is derived.

Moreover, as discussed above, the KDM is merely generated by a content provider and received from the playback device. There is no teaching or suggestion that the KDM is generated from a mating key generator using the rights key, allegedly the first derivative key.

The Examiner alleges that "Kocher further discloses the rights key includes a content identifier" (Final Office Action, page 8). As discussed above, since the KDM is not generated using the rights key, even if the rights key was to include a content identifier, the rights key cannot correspond to the mating key generator, as delineated in the claim.

Furthermore, the claim recites "to generate a mating key from a mating key generator using the first derivative key" such that the mating key generator and the first derivative key are separate and distinct elements in the claim. Given that the Examiner alleges that the rights key corresponds to the first derivative keys as well as the mating key generator, Kocher fails to disclose these elements of the claim.

In addition, Kocher does not describe a third process block configured to recover a control word, allegedly the CDK, by decrypting an encrypted control word using the mating key, allegedly the KDM. The KDM does not appear to be used for any decryption operations (Kocher, col. 11, lines 33-65; Figure 5).

The Examiner alleges that "the KDM (i.e. mating key) is used to identify the rights key, which is then used to transform the CDK and decrypt the content (i.e. decrypt the control word)" (Final Office Action, page 9). Applicant respectfully disagrees.

Applicant respectfully submits Kocher merely discloses using the CDK to decrypt the content (Kocher, col. 11, lines 64-65; Figure 5). Accordingly, the CDK is used to decrypt the content and not the KDM, as alleged by the Examiner.

Furthermore, the content in Kocher is merely digital content is "a digital representation of human-interpretable material, such as pictures, audio tracks, video segment text" (Kocher, col. 8, lines 1-6). In contrast, a control word is used for descrambling scrambled content (See Specification, page 38, for further details). Thus, the digital content in Kocher cannot be a control word, as alleged by the Examiner.

Hence, Applicant respectfully submits that claim 22 is in condition for allowance.

D. Claim 28

With respect to claim 28, similar to the arguments presented above, Kocher does not describe the recovery of the plurality of control words (CDKs) using the plurality of mating keys (KDMs). Applicant incorporates the arguments made above and respectfully requests the Examiner to withdraw the rejection or to provide ample evidence in support of the rejection. Withdrawal of the outstanding §102(b) rejection is respectfully requested.

With respect to claims 2-12, 14, 18-21, 23 and 27, Applicant respectfully traverses the outstanding §102(b) rejection because a *prima facie* case of anticipation has not been established for these claims. Based on the dependency of the above-identified claims on independent claims 1, 13 and 22, which are believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traversing the rejection is necessary. For illustrative purposes, however, we shall discuss a few of these claims to illustrate that Kocher clearly does not anticipate these claims.

In light of the foregoing, Applicant respectfully requests that the Examiner withdraw the outstanding §102(b) rejection.

Rejection Under 35 U.S.C. § 103

Claims 26 and 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher. Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988).* Herein, Kocher does not teach or suggest all of the claim limitations and incorporates the arguments set forth above.

Withdrawal of the outstanding §103 rejection is respectfully requested.

Furthermore, claims 15-17, 24, 25 and 30-32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kocher in view of Wasilewski (U.S. Patent Publication No. 2004/003008). Herein, Applicant respectfully submits that neither Kocher nor Wasilewski, alone or in combination, describe or suggest all of the claim limitations set forth in these claims, especially those limitations denoted above in traversing the outstanding §102(b) rejection. Applicant incorporates these arguments by reference. Also, based on the dependency of the above-identified claims on independent claims 1, 13, 22 and 28, which are believed by Applicant to be in condition for allowance, no further discussion as to the grounds for traversing the rejection is necessary.

Applicant respectfully requests that the Examiner withdraw the rejection of claims 15-17, 24, 25 and 30-32 under 35 U.S.C. § 103(a) as being unpatentable over the combined teachings of Kocher and Wasilewski.

Conclusion

Applicant respectfully requests that the corrected claims with amended claim identifiers be accepted and entered.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: December 23, 2008

By /William W. Schaal /
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)